

23



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/558,022	04/25/2000	Takatoshi Ono	NAK1-BK74	9324

21611 7590 01/31/2006

SNELL & WILMER LLP
600 ANTON BOULEVARD
SUITE 1400
COSTA MESA, CA 92626

EXAMINER

SHERKAT, AREZOO

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 01/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Advisory Action
Before the Filing of an Appeal Brief**

Application No.

09/558,022

Applicant(s)

ONO ET AL.

Examiner

Arezoo Sherkat

Art Unit

2131

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 19 January 2006 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☐ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.
b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
(a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
(b) ☐ They raise the issue of new matter (see NOTE below);
(c) ☒ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
(d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
The status of the claim(s) is (or will be) as follows:
Claim(s) allowed: _____.
Claim(s) objected to: _____.
Claim(s) rejected: 1-10.
Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:
See Note.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____.
13. ☐ Other: _____.

CEL
Primary Examiner
APR 13
1/29/06

Applicant argues that "Wasilewski does not disclose a data usage controlling apparatus that decrypts the encrypted condition information using the type 2 key and includes second updating means for updating the type 1 key in the storage unit in accordance with the usage of the read main data and second encrypting means for encrypting the new type 2 key using the updated type 1 key and replacing the encrypted type 2 key on the recording medium with the encrypted new type 2 key.

Examiner responds that Wasilewski discloses that MSK (i.e., type 1 key) changes/updates in the order of once a day or once a month in SABER 20 to be transferred to STU 90 (Col. 10, lines 1-12). Wasilewski also discloses encrypting the new type 2 key (i.e., control words that are used in the first level of encryption and are changed every few seconds - Col. 8, lines 48-60) using the updated type 1 key (i.e., MSK that are updated in the order of once a day or once a month - Col. 10, lines 1-5) and replacing the encrypted type 2 key on the recording medium with the encrypted new type 2 key (Col. 9, lines 12-67 and Col. 10, lines 13-67).

Wasilewski discloses that the clear control word, other data (e.g., system wide pay per view access, copy protection, i.e., the usage information), and the MSK are concatenated together. This concatenation is then hashed, using a one-way hash algorithm, such as well-known Message Digest (MD5) algorithm, to produce a MAC. The MD5 hash produces an output value from which it is computationally infeasible to discover the input value to the hash algorithm. The MAC is appended to the encrypted control word. The producer of the MAC (i.e., the SABER 20) must know both the pre-encrypted control word and the MSK to produce a proper output hash value. The resulting hash value is transmitted to the STU 90, along with the encrypted control work in the ECM (Col. 9, lines 30-46)